22. (Currently amended) A computer-readable medium as recited in Claim 19, comprising further sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of creating and storing the balanced binary tree by creating and storing a stack of h elements wherein the i^{th} element of said stack stores a state datum for the i^{th} node on a path from a root node of the tree to the leaf node.

23. (Currently amended) An apparatus as recited in Claim 20, further comprising creating and storing the balanced binary tree by creating and storing a stack of h elements wherein the i^{th} element of said stack stores a state datum for the i^{th} node on a path from a root node of the tree to the leaf node.

24. (Currently amended) An apparatus as recited in Claim 21, wherein the sequences of instructions comprise further sequences of instructions which, when executed by the processor, cause the processor to perform the steps of creating and storing the balanced binary tree by creating and storing a stack of h elements wherein the i^{th} element of said stack stores a state datum for the i^{th} node on a path from a root node of the tree to the leaf node.

25. (New) A computer-readable medium as recited in Claim 22, comprising further sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of creating and storing a state value for a leaf node comprises the steps of computing and storing a state value for the leaf node that is unique with respect to any other state value that is computed at any other time for any other leaf node of the tree.

26. (New) A computer-readable medium as recited in Claim 19, wherein each leaf node stores m bits of state information, wherein m is a multiple of twelve.

27. (New) A computer-readable medium as recited in Claim 19, comprising further sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

creating and storing $m=3n$ bits of state information in each leaf node comprising a concatenation of three n bit quantities $z \mid y \mid x$, wherein n is a multiple of four;

computing the first non-linear function a and the second non-linear function b as the composition of a diffusion function d with the nonlinear "confusion" functions f and g, wherein $a = f \circ d$ and $b = g \circ d$ and wherein

$f(z \mid y \mid x) = 2z \mid S(R(S(R(y)))) \mid L(S(L(S(x))))$

$g(z \mid y \mid x) = 2z+1 \mid L(S(L(S(y)))) \mid S(R(S(R(\neg x)))))$

$d(z \mid y \mid x) = z \mid x + y + z \mid 2x + y + z$

$c(z \mid y \mid x) = x \oplus y$

wherein integer addition modulo two is denoted as +, bitwise exclusive-or is denoted as $\oplus$, and bitwise complementation is denoted as $\neg$;

wherein the R denotes rotation by $n/4$ bits to in a direction of a least significant bit and L denotes rotation by $n/4$ bits in a direction of a most significant bit; and

wherein a nonlinear function S comprises a lookup in a key-dependent substitution table.

28. (New) A computer-readable medium as recited in Claim 19, wherein the third function comprises computing a linear reduction of $2n$ bits of the state value to n bits thereof.

29. (New) A computer-readable medium as recited in Claim 27, wherein the third function comprises computing a bitwise Boolean exclusive OR of x and y.

30. (New) A computer-readable medium as recited in Claim 27, comprising further sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of creating and storing the substitution table

S by selecting four invertible functions and storing the four invertible functions in a concatenated form.

31. (New) A computer-readable medium as recited in Claim 27, comprising further sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of computing functions *f* and *g* in seven instructions of a central processing unit that can issue two instructions simultaneously, by using five registers to store values of *x*, *y*, *z*, a temporary variable, and a pointer to the substitution table *S*.

32. (New) A computer-readable medium as recited in Claim 27, wherein the substitution table *S* comprises an array of key dependent pseudorandom integer values.

33. (New) A computer-readable medium as recited in Claim 27, wherein the substitution table *S* comprises an array of 256 key dependent pseudorandom 32-bit unsigned integer values.

34. (New) A computer-readable medium as recited in Claim 19, comprising further sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of creating and storing a key for use by the first non-linear function and the second non-linear function, wherein the key comprises a table of key dependent pseudorandom values.

35. (New) A computer-readable medium as recited in Claim 19, comprising further sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of creating and storing, once and at a time prior to receiving the location value, a key for use by the first non-linear function and the second non-linear function, wherein the key comprises a table of key dependent pseudorandom values.

36. (New) A computer-readable medium as recited in Claim 19, comprising further sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of creating and storing a key in the form of a plurality of pseudo-randomly selected invertible functions, wherein each of the invertible functions maps an 8-bit portion of the state value to an 8-bit quantity for use as a substitute portion of the state value.

37. (New) A computer-readable medium as recited in Claim 19, wherein the pseudo-randomly selected invertible functions are stored in a plurality of substitution tables, and wherein the plurality of substitution tables are generated by:
setting each of the plurality of substitution tables equal to the identity function;
for each element of each of the plurality of substitution tables, swapping said element with another element of such table in a key-dependent manner, and also performing the same swapping operation on each table that has been previously been generated.

38. (New) An apparatus as recited in Claim 23, further comprising creating and storing a state value for a leaf node comprises the steps of computing and storing a state value for the leaf node that is unique with respect to any other state value that is computed at any other time for any other leaf node of the tree.

39. (New) An apparatus as recited in Claim 20, wherein each leaf node stores m bits of state information, wherein m is a multiple of twelve.

40. (New) An apparatus as recited in Claim 20, further comprising:
means for creating and storing $m=3n$ bits of state information in each leaf node comprising a concatenation of three n bit quantities $z \mid y \mid x$, wherein n is a multiple of four;

means for computing the first non-linear function *a* and the second non-linear function *b* as the composition of a diffusion function *d* with the nonlinear "confusion" functions *f* and *g*, wherein $a = f \circ d$ and $b = g \circ d$ and wherein

$f(z \mid y \mid x) = 2z \mid S(R(S(R(y)))) \mid L(S(L(S(x))))$

$g(z \mid y \mid x) = 2z+1 \mid L(S(L(S(y)))) \mid S(R(S(R(\neg x))))$

$d(z \mid y \mid x) = z \mid x + y + z \mid 2x + y + z$

$c(z \mid y \mid x) = x \oplus y$

wherein integer addition modulo two is denoted as +, bitwise exclusive-or is denoted as $\oplus$, and bitwise complementation is denoted as $\neg$;

wherein the *R* denotes rotation by *n*/4 bits to in a direction of a least significant bit and *L* denotes rotation by *n*/4 bits in a direction of a most significant bit; and

wherein a nonlinear function *S* comprises a lookup in a key-dependent substitution table.

41. (New) An apparatus as recited in Claim 20, wherein the third function comprises computing a linear reduction of $2n$ bits of the state value to n bits thereof.

42. (New) An apparatus as recited in Claim 40, wherein the third function comprises computing a bitwise Boolean exclusive OR of *x* and *y*.

43. (New) An apparatus as recited in Claim 40, further comprising means for creating and storing the substitution table *S* by selecting four invertible functions and storing the four invertible functions in a concatenated form.

44. (New) An apparatus as recited in Claim 40, further comprising means for computing functions *f* and *g* in seven instructions of a central processing unit that can issue two instructions simultaneously, by using five registers to store values of *x*, *y*, *z*, a temporary variable, and a pointer to the substitution table *S*.

45. (New) An apparatus as recited in Claim 40, wherein the substitution table *S* comprises an array of key dependent pseudorandom integer values.

46. (New) An apparatus as recited in Claim 40, wherein the substitution table *S* comprises an array of 256 key dependent pseudorandom 32-bit unsigned integer values.

47. (New) An apparatus as recited in Claim 20, further comprising means for creating and storing a key for use by the first non-linear function and the second non-linear function, wherein the key comprises a table of key dependent pseudorandom values.

48. (New) An apparatus as recited in Claim 20, further comprising means for creating and storing, once and at a time prior to receiving the location value, a key for use by the first non-linear function and the second non-linear function, wherein the key comprises a table of key dependent pseudorandom values.

49. (New) An apparatus as recited in Claim 20, further comprising means for creating and storing a key in the form of a plurality of pseudo-randomly selected invertible functions, wherein each of the invertible functions maps an 8-bit portion of the state value to an 8-bit quantity for use as a substitute portion of the state value.

50. (New) An apparatus as recited in Claim 20, wherein the pseudo-randomly selected invertible functions are stored in a plurality of substitution tables, and wherein the plurality of substitution tables are generated by means for:
setting each of the plurality of substitution tables equal to the identity function;
for each element of each of the plurality of substitution tables, swapping said element with another element of such table in a key-dependent manner, and also performing the same swapping operation on each table that has been previously been generated.

51. (New) An apparatus as recited in Claim 24, wherein the sequences of instructions comprise further sequences of instructions which, when executed by the processor, cause the processor to perform the steps of creating and storing a state value for a leaf node comprises the steps of computing and storing a state value for the leaf node that is unique

with respect to any other state value that is computed at any other time for any other leaf node of the tree.

52. (New) An apparatus as recited in Claim 21, wherein each leaf node stores m bits of state information, wherein m is a multiple of twelve.

53. (New) An apparatus as recited in Claim 21, wherein the sequences of instructions comprise further sequences of instructions which, when executed by the processor, cause the processor to perform the steps:

creating and storing $m=3n$ bits of state information in each leaf node comprising a concatenation of three n bit quantities $z \mid y \mid x$, wherein n is a multiple of four;

computing the first non-linear function a and the second non-linear function b as the composition of a diffusion function d with the nonlinear "confusion" functions f and g, wherein $a = f \circ d$ and $b = g \circ d$ and wherein

$f(z \mid y \mid x) = 2z \mid S(R(S(R(y)))) \mid L(S(L(S(x))))$

$g(z \mid y \mid x) = 2z+1 \mid L(S(L(S(y)))) \mid S(R(S(R(\neg x)))))$

$d(z \mid y \mid x) = z \mid x+y+z \mid 2x+y+z$

$c(z \mid y \mid x) = x \oplus y$

wherein integer addition modulo two is denoted as +, bitwise exclusive-or is denoted as $\oplus$, and bitwise complementation is denoted as $\neg$;

wherein the R denotes rotation by $n/4$ bits to in a direction of a least significant bit and L denotes rotation by $n/4$ bits in a direction of a most significant bit; and

wherein a nonlinear function S comprises a lookup in a key-dependent substitution table.

54. (New) An apparatus as recited in Claim 21, wherein the third function comprises computing a linear reduction of $2n$ bits of the state value to n bits thereof.

55. (New) An apparatus as recited in Claim 53, wherein the third function comprises computing a bitwise Boolean exclusive OR of x and y.

56. (New) An apparatus as recited in Claim 53, wherein the sequences of instructions comprise further sequences of instructions which, when executed by the processor, cause the processor to perform the steps of creating and storing the substitution table *S* by selecting four invertible functions and storing the four invertible functions in a concatenated form.

57. (New) An apparatus as recited in Claim 53, wherein the sequences of instructions comprise further sequences of instructions which, when executed by the processor, cause the processor to perform the steps of computing functions *f* and *g* in seven instructions of a central processing unit that can issue two instructions simultaneously, by using five registers to store values of *x*, *y*, *z*, a temporary variable, and a pointer to the substitution table *S*.

58. (New) An apparatus as recited in Claim 53, wherein the substitution table *S* comprises an array of key dependent pseudorandom integer values.

59. (New) An apparatus as recited in Claim 53, wherein the substitution table *S* comprises an array of 256 key dependent pseudorandom 32-bit unsigned integer values.

60. (New) An apparatus as recited in Claim 21, wherein the sequences of instructions comprise further sequences of instructions which, when executed by the processor, cause the processor to perform the steps of creating and storing a key for use by the first non-linear function and the second non-linear function, wherein the key comprises a table of key dependent pseudorandom values.

61. (New) An apparatus as recited in Claim 21, wherein the sequences of instructions comprise further sequences of instructions which, when executed by the processor, cause the processor to perform the steps of creating and storing, once and at a time prior to receiving the location value, a key for use by the first non-linear function and the second non-linear function, wherein the key comprises a table of key dependent pseudorandom values.

62. (New) An apparatus as recited in Claim 21, wherein the sequences of instructions comprise further sequences of instructions which, when executed by the processor, cause the processor to perform the steps of creating and storing a key in the form of a plurality of pseudo-randomly selected invertible functions, wherein each of the invertible functions maps an 8-bit portion of the state value to an 8-bit quantity for use as a substitute portion of the state value.

63. (New) An apparatus as recited in Claim 21, wherein the pseudo-randomly selected invertible functions are stored in a plurality of substitution tables, and wherein the plurality of substitution tables are generated by instructions for performing the steps of:

setting each of the plurality of substitution tables equal to the identity function;

for each element of each of the plurality of substitution tables, swapping said element with another element of such table in a key-dependent manner, and also performing the same swapping operation on each table that has been previously been generated.